IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of: David John Craft et al.	§	Confirmation No.: 7981
Serial Number: 10/601,374	§	
	§	Group Art Unit: 2136
Filed: June 23, 2003	§	
For: SECURITY ARCHITECTURE FOR SYSTEM ON CHIP	§	Examiner: Carlton Johnson

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 37 C.F.R. § 1.8, I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office at www.uspto.gov .

on: 23 February 2009

/Patrick E. Caldwell/
Patrick E. Caldwell

Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICANTS' APPEAL BRIEF

Applicant-inventors ("Applicants") and assignee International Business Machines Corporation respectfully submit the present brief in support of the patentability of the claims of the above-referenced application.

I. REAL PARTY IN INTEREST

The real party in interest is International Business Machines Corporation, of Armonk, New York, assignee of the interests in the invention from the named inventors.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

Claims 22-37 are pending. Of these, Claims 22 and 31 are independent Claims. Claims 1-21 have been canceled. Applicants appeal the Examiner's rejections of Claims 22-37 under 35 U.S.C. §103(a).

IV. STATUS OF AMENDMENTS

The Claims stand as amended in the Response to an Office Action dated March 13, 2007.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Modern microprocessors, particularly networked processors, are increasingly equipped with or adapted for security mechanisms to provide authentication and encryption functions to be performed in the constituent networked processors. *See* Application, Page 1, Lines 9-15. One conventional method provides a hardware mechanism to ensure that the initial operating system image has not been tampered with. *See* Application, Page 2, Lines 5-7. This approach, however, depends on the Operating System (OS) to maintain system integrity once the system has been started. *See* Application, Page 2, Lines 7-9. Therefore, this approach suffers from the disadvantage that Operating Systems are often very insecure. *See* Application, Page 2, Lines 9-14.

Another conventional system provides a separate security chip in the computer system, capable of providing the authentication, encryption, and key management functions, such as

those specified by the trusted computing alliance (TCA™). *See* Application, Page 2, Lines 15-20. A separate chip has the advantage that its interface protocols can be limited to security functions, which can make it very difficult to mount a software attack on such a chip. *See* Application, Page 2, Lines 20-23. However, because the security chip is separate from the microprocessor, it is relatively easy to monitor the interfaces and circumvent the protocols, and therefore does not provide good protection for implementing a secure boot function because the authenticated operating system image can relatively easily be replaced. *See* Application, Page 2, Lines 23-29.

Another conventional system provides an integrated security unit connected to the processor input/output (I/O) or the memory interface. *See* Application, Page 2, Lines 30-33. Because these integrated security devices provide the authentication and/or encryption functions on the processor chip, this unit is not easily monitored, and therefore provides a higher degree of protection than a separate security chip. *See* Application, Page 3, Lines 1-6. However, this arrangement suffers from significant disadvantages in that the security unit can occupy a significant silicon area on the processor chip, which is typically implemented in significantly more expensive technology and that such a unit, if it is to be realized at a reasonable cost (area), can provide basic functionality only. *See* Application, Page 3, Lines 6-12.

The present invention, defined in Claims 22-37, solves these and other problems by providing a novel method and apparatus for secure processing, particularly authenticating code and/or data and providing a protected environment for execution. *See* Application, Page 19, Lines 4-6. The novel method and apparatus dynamically partitions and un-partitions a local store for the authentication of code or data. *See* Application, Page 19, Lines 6-8. The local store is partitioned into an isolated and non-isolated section and code or data is loaded into the isolated

section. *See* Application, Page 19, Lines 8-10. The code or data is authenticated in the isolated section of the local store and then executed. *See* Application, Page 19, Lines 10-12. After execution, the memory within the isolated region is erased and de-partitioned. *See* Application, Page 19, Lines 12-16.

The Claims embody the invention as follows, as indicated in the Independent Claims shown below with illustrative citations to page and line numbers in the Original Application designated in curved braces ("{}"):

Claim 22: A secure processing system, comprising: {Page 5, Lines 14-17}

a main processor unit (MPU) coupled to a processor bus; {Page 5, Line 31}

an attached processor complex (APC) coupled to the processor bus and comprising: {Page 5, Lines 17-27}

a local store configured to store computer instructions and data; {Page 5, Lines 15-16}

an attached processor unit (APU) coupled to the local store; {Page 5, Lines 18-19}

wherein the APC is configured to receive commands from the MPU via the processor bus, to store a cryptographic master key, and to operate in a non-isolated state and an isolated state; and {Page 6, Lines 1-15; 23-25}

wherein in response to a LOAD command received from the MPU, the APC is configured to transition from the non-isolated state to the isolated state, to partition the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU, to transfer a set of computer instructions or data into the isolated section of the local store, and to use the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic key. {Page 7; Lines 3-20}

Claim 31: A method for carrying out secure processing, comprising:

providing a main processor unit (MPU), a processor bus, and an attached processor complex (APC), wherein the APC comprises a local store configured to store computer instructions and data and an attached processor unit (APU) coupled to the local store; {Page 5, Lines 15-31}

configuring the MPU to drive a LOAD command on the processor bus in the event secure processing is required; {Page 7, Lines 3-7}

coupling the MPU to the processor bus; {Page 5, Line 31}

configuring the APC to receive the LOAD command via the processor bus, to store a cryptographic master key, and to operate in a non-isolated state and an isolated state; {Page 6, Lines 1-9}

configuring the APC to respond to a received LOAD command by:

transitioning from the non-isolated state to the isolated state; {Page 5, Lines 15-17}

partitioning the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU; {Page 6, Lines 16-26}

transferring a set of computer instructions or data into the isolated section of the local store; {Page 7, Lines 10-14}

using the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic key; and {Page 7, Lines 10-14}

coupling the APC to the processor bus. {Page 6, Lines 5-7}

VI. GROUNDS OF REJECTION TO BE REVIEWED

Whether Claims 22-27 and 29-36 are patentable over Ellison et al. (US 7,082,615)("Ellison") in view of Smeets et al. (US 6,769,062)("Smeets").

Whether Claims 28 and 37 are patentable over Ellison and Smeets in view of Worley Jr. et al. (US PGPUB 2002/0194389)("Worley").

VII. ARGUMENT

A. Grouping of Claims

Claims 22 and 31 are independent. For purposes of this appeal, Applicants consider each of the independent Claims, and their respective dependent Claims, as separate groups. Thus, the groups of Claims are 22-30 and 31-37.

B. Summary of Pertinent Prosecution

Applicants filed the present application on June 23, 2003, with 21 claims.

The Examiner mailed the first Office Action on November 29, 2006 ("First Action"), rejecting Claims 1-4, 6-8, and 10- 21 under 35 U.S.C. §103(a) as allegedly unpatentable over Ellison in view of Worley. Similarly, the Examiner rejected Claims 5 and 9 based on the combination of Ellison and Worley in view of Dahan et al. (US PGPUB 2003/0140244)("Dahan").

Applicants responded to the First Action on March 13, 2007 ("First Response"), cancelling Claims 1-21 and adding new Claims 22-37.

The Examiner mailed the First Final Action on June 1, 2007 ("First Final Action"). In the First Final Action, the Examiner rejected Claims 22-27 and 29-36 under 35 U.S.C. §102(e) as allegedly anticipated by Ellison. The Examiner also rejected Claims 28 and 37 under 35 U.S.C. §103(a) as allegedly unpatentable over Ellison in view of Worley.

Applicants appealed, filing an Appeal Brief ("First Appeal Brief") on December 28, 2007. Applicants argued that Ellison does not teach each and every element of the Claims. Specifically, Applicants asserted that Ellison does not teach, disclose, or suggest "*in response to* a LOAD command received from the MPU, the APC is configured . . . to partition the local store into a

general access section accessible by the MPU and an isolated section accessible only by the APU," as recited in Claim 22, or "configuring the APC to respond to a received LOAD command by: . . . partitioning the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU," as recited in Claim 31.

In response to the First Appeal Brief, the Examiner reopened prosecution on the merits in a non-final Office Action on March 18, 2008 ("Second Action"). In the Second Action, the Examiner rejected Claims 22-27 and 29-36 under 35 U.S.C. §103(a) as allegedly unpatentable over Ellison in view of Smeets. The Examiner also rejected Claims 28 and 37 under 35 U.S.C. §103(a) as allegedly unpatentable over Ellison-Smeets in view of Worley.

Applicants responded to the Second Action on June 18, 2008 ("Second Response"), arguing that none of the cited references, alone or in combination, teach the elements recited in the pending Claims. Specifically, Applicants asserted that the Examiner's proposed combination does not partition the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU *in response to* a LOAD command. Instead, the Examiner's proposed combination teaches accessing a static, pre-existing, permanent isolated section.

The Examiner maintained the rejections of the Second Action in a Second Final Action dated October 23, 2008 ("Second Final Action"). The Examiner also responded to Applicants' Second Response, described in more detail below.

This appeal followed.

C. The Examiner's Rejections

While Applicants traverse the Examiner's rejections in their entirety, Applicants here highlight the aspects of the Examiner's rejections most relevant to the instant appeal.

Regarding Claim 22, to support the rejections under Section 103(a), the Examiner cites Ellison as showing "in response to a LOAD command received from the MPU . . . the APC is configured to transition from the non-isolated state to the isolated state." Second Final Action, Page 5 (*citing* Ellison, col. 3, lines 43-45; col. 4, lines 16-22). The Examiner also cites Ellison as showing, "wherein to partition the local store into a general access section and an isolated section." Second Final Action, Page 5 (*citing* Ellison, col. 4, lines 16-22)." The Examiner offers Smeets as showing "wherein a general access section accessible by the MPU and an isolated section accessible only by the APU", which the Examiner admits is missing from Ellison. Second Final Action, Pages 5-6 (*citing* Smeets, Fig. 1, items 18, 20; col. 2, lines 2-5, 19-23; col. 3, lines 18-20, 26-28, and 58-60). The Examiner asserts that it would be obvious "to modify Ellison to enable the capability for a general access section accessible by the MPU and an isolated section accessible only by the APU as taught by Smeets." Second Final Action, Page 6.

Regarding Claim 31, to support the rejections under Section 103(a), the Examiner cites Ellison as showing "configuring the APC to respond to a received LOAD command by: transitioning from the non-isolated state to the isolated state." Second Final Action, Page 0 (*citing* Ellison, col. 5, lines 5-10). The Examiner also cites Ellison as showing, "wherein to partition the local store into a general access section and an isolated section." Second Final Action, Page 9 (*citing* Ellison, col. 4, lines 16-22)." The Examiner offers Smeets as showing "wherein a general access section accessible by the MPU and an isolated section accessible only by the APU", which the Examiner again admits is missing from Ellison. Second Final Action, Pages 9-10 (*citing* Smeets, Fig. 1, items 18, 20; col. 2, lines 2-5, 19-23; col. 3, lines 18-20, 26-28, and 58-60). The Examiner asserts that it would be obvious "to modify Ellison to enable the

capability for a general access section accessible by the MPU and an isolated section accessible only by the APU as taught by Smeets." Second Final Action, Page 10.

D. The Examiner's Rejections Were Procedurally and Factually in Error

1. The Form and Content of the Examiner's Rejections under Section 103 Were Improper and Insufficient

a. Legal Requirements for an Obviousness Rejection

The obligation of the examiner to produce reasoning and evidence in support of obviousness is clearly defined at M.P.E.P. §2142:

> The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.
>
> M.P.E.P. §2142.

To make a prima facie case, the Examiner must perform certain established inquiries: "Obviousness is a question of law based on underlying factual inquiries." M.P.E.P. §2141(II). These factual inquiries include determining the scope and content of the prior art, "Ascertaining the differences between the claimed invention and the prior art;" and "Resolving the level of ordinary skill in the pertinent art." M.P.E.P. §2141(II)(citing Graham v. John Deere Co., 383 U.S. 1, at 17-18, 148 USPQ 459, at 467 (1966)).

These factual inquiries required to establish a *prima facie* case are not optional: "Office personnel fulfill the critical role of factfinder when resolving the Graham inquiries . . . When making an obviousness rejection, Office personnel must therefore ensure that the written record includes findings of fact concerning the state of the art and the teachings of the references applied." M.P.E.P. §2141(II)(emphasis added). Thus, the Examiner *must* make these three factual inquiries in order to support a proper Section 103 rejection. Without these factual

inquiries, the Section 103 rejection cannot stand: "Factual findings made by Office personnel are the necessary underpinnings to establish obviousness." M.P.E.P. §2141(II).

Furthermore, in undertaking the mandatory factual inquiries, the Examiner must contemplate the Claims as a whole: "In view of all factual information, the examiner must then make a determination whether the claimed invention 'as a whole' would have been obvious at that time to that person." M.P.E.P. §2141. Moreover, the Examiner must consider each and every element in the pending Claims: "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970); M.P.E.P. §2143.03.

As stated in the MPEP, "The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious." M.P.E.P. §2142. The Examiner's rejections in this case fail to ascertain all of the differences between the claimed invention and the prior art and fail to show how those differences would have been obvious. "[R]ejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006); M.P.E.P. §2142. Applicants respectfully submit that the Examiner has not met this burden and has therefore failed to establish a *prima facie* case of obviousness.

b. The Examiner has failed to establish a *prima facie* case of obviousness

As described above, the Examiner rejects Claims 1-27 and 29-36 under 35 U.S.C. §103(a) as allegedly unpatentable over Ellison in view of Smeets and Ellison-Smeets in view of Worley. *See* Second Final Action, Pages 4, 11. Applicant respectfully submits that these rejections are in error and should be withdrawn.

In order to establish a *prima facie* case of obviousness, the Examiner must consider each and every element of each Claim, and consider whether each Claim as a whole would have been obvious. *See* M.P.E.P. §§2141, 2141.03. Claim 22 recites, in relevant part, "*in response to* a LOAD command received from the MPU, the APC is configured . . . to partition the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU". (Emphasis added.) The Examiner has failed to properly consider this element and has failed to show why it would have been obvious.

Instead, the Examiner asserts that it would be obvious "to modify Ellison to enable the capability for a general access section accessible by the MPU and an isolated section accessible only by the APU as taught by Smeets." Second Final Action, Page 10. Even if that were true, a fact Applicants do not concede, the Examiner's assertion still fails to show that the isolated section is created *in response to* a LOAD instruction. Nor does the assertion indicate why creating the partition in response to the LOAD instruction would be obvious.

Further, Applicants respectfully submit that neither Ellison, Smeets, nor Worley, alone or in any combination teach each and every element of the Claims. Specifically, the cited references do not teach, disclose, or suggest "wherein *in response to* a LOAD command received from the MPU, the APC is configured . . . to partition the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU," as recited in Claim 22, or "configuring the APC *to respond to* a received LOAD command by: . . . partitioning the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU," as recited in Claim 31. (Emphasis added.)

Regarding Claims 22 and 31, the Examiner cites Ellison as showing "in response to a LOAD command received from the MPU . . . the APC is configured to transition from the non-

isolated state to the isolated state." Second Final Action, Page 5 (*citing* Ellison, col. 3, lines 43-45; col. 4, lines 16-22). The Examiner also cites Ellison as showing, "wherein to partition the local store into a general access section and an isolated section." Second Final Action, Page 5 (*citing* Ellison, col. 4, lines 16-22)." Applicants note that the Examiner did not cite "in response to a LOAD command received from the MPU . . . partition[ing] the local store into a general access section and an isolated section," as recited in the Claim.

Applicants noted this missing element in the First Appeal Brief and the Second Response. *See*, *e.g.*, First Appeal Brief, Pages 8-9; Second Response, Page 5. Nevertheless, in the Second Final Action, the Examiner attempts to finesse this element: "The Ellison prior art does not specifically disclose the LOAD command but the prior art discloses that a command is used to invoke the isolated execution *state*." Second Final Action, Page 2, Para 3.1 (*citing* Ellison, Fig. 1C; col. 4, lines 40-45, 63-65; col. 3, lines 43-49)(emphasis added). Here, it appears that Examiner wrongly equates "the isolated execution state" with the "isolated section accessible only by the APU."

The Examiner also asserts, "The Ellison prior art discloses that the isolated region is configured (established) by the execution of the instruction to invoke the isolated operational state." Second Final Action, Page 3, Para 3.2 (*citing* Ellison, col. 4, lines 63-65; col. 3, lines 43-49). Ellison, however, flatly contradicts the Examiner's statement.

Specifically, Ellison recites, "The isolated execution *mode* is initialized using a privileged instruction in the processor, combined with the processor nub 52." Ellison, col. 3, lines 43-45 (emphasis added). And, "The OS nub 16 and the processor nub 18 are instances of an OS executive (OSE) and a processor executive (PE), respectively. The OSE and PE are part of executive entities that operate in a secure environment associated with the isolated area 70 and

the isolated execution mode." Ellison, col. 3, lines 16-22. Together, these citations show that Ellison actually teaches away from the elements related to "in response to a LOAD command received from the MPU" as recited in the pending Claims.

That is, Ellison distinguishes between its "isolated execution mode" and its pre-partitioned "isolated area": in the "isolated execution mode," "The processor nub loader 52 verifies and loads a ring-0 nub software module (e.g., processor nub 18) into the isolated area." Ellison, col. 3, lines 45-47. That is, the Ellison "isolated area" is not configured or established *in response to* invoking the "isolated execution mode"—the Ellison "isolated area" already exists prior to the "isolated execution mode." More particularly, "The logical operating architecture 50 [of Ellison] has two modes of operation: normal execution mode and isolated execution mode." Ellison, col. 3, lines 4-6. The Ellison architecture contains "rings" that are perpetually partitioned into "normal execution" portion and an "isolated execution" portion, for example: "Ring-0 10 includes two portions: a normal execution Ring-0 11 and an isolated execution Ring-O 15." Ellison, col. 3, lines 9-10.

Thus, because Ellison's isolated execution portion is perpetual, Ellison affirmatively teaches away from an "isolated section accessible only by the APU" that is partitioned "in response to a LOAD command," as recited in the claims. For at least this reason, Ellison affirmatively teaches away from this element of the Claims, and therefore cannot support a proper rejection under Section 103.

Notwithstanding the identified missing element, the Examiner does admit that "Ellison does not specifically disclose a general access section accessible by the MPU and an isolated section accessible only by the APU." Second Final Action, Page 5. As described above, the Examiner offers Smeets to provide this element. *See* Second Final Action, Page 5. However,

Applicants respectfully submit that nowhere does Smeets show an "isolated section accessible only by the APU" that is partitioned "in response to a LOAD command," as recited in the Claims. Nor does the Examiner assert that Smeets provides this missing element.

Accordingly, even if Ellison did not affirmatively preclude this element, Smeets fails to supply it, and the Examiner's proposed combination of Ellison and Smeets fails to teach each and every element as recited in Claims 22 and 31. In fact, as described above, the Examiner's proposed combination actually teaches away from an "isolated section accessible only by the APU" that is partitioned "in response to a LOAD command," because each reference teaches a pre-existing, static partition, not a dynamic partition created in response to a LOAD command. Therefore the Examiner's proposed combination teaches away from the Claims as recited, thereby also providing evidence that the Claims as recited are not obvious in light of the cited art.

Applicants therefore respectfully submit that independent Claims 22 and 31 are patentable over Ellison and Smeets, alone or in any combination. Applicants respectfully request that the rejections of Claims 22 and 31 be withdrawn and that Claims 22 and 31 be allowed.

Claims 23-27 and 29-30 depend on and further limit Claim 22. Claims 32-36 depend on and further limit Claim 31. As such, Applicants respectfully submit that these dependent Claims are also patentable over Ellison and Smeets, for at least the reasons as indicated above. Accordingly, Applicants respectfully request that the rejections of dependent Claims 23-27, 29-30, and 32-36 also be withdrawn and that Claims 23-27, 29-30, and 32-36 be allowed.

As described above, the Examiner rejects Claims 28 and 37 under 35 U.S.C. §103(a) as allegedly unpatentable over Ellison-Smeets in view of Worley. *See* Second Final Action, Page 11. Applicants respectfully submit that these rejections are in error and should be withdrawn.

More particularly, as described above, Ellison-Smeets wholly fails to teach, disclose, or suggest, and in fact teaches away from, "wherein in response to a LOAD command received from the MPU, the APC is configured . . . to partition the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU," as recited in Claim 22 (from which Claim 28 depends), or "configuring the APC to respond to a received LOAD command by: . . . partitioning the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU," as recited in Claim 31 (from which Claim 37 depends).

The Examiner offers no suggestion that Worley supplies this element missing from Ellison-Smeets. *See* Second Final Action, Pages 11-14. Instead, the Examiner admits that "Ellison does not specifically disclose whereby to authenticate another set of computer instructions or data" and offers Worley to provide this element. *See* Second Final Action, Page 14. However, Applicants respectfully submit that nowhere does Worley show an "isolated section accessible only by the APU" that is partitioned "in response to a LOAD command," as recited in the independent claims from which Claims 28 and 37 depend.

Accordingly, even if Ellison did not affirmatively preclude this element, both Smeets and Worley fail to supply it, and the Examiner's proposed combination of Ellison, Smeets, and Worley fails to teach, or even suggest, each and every element as recited in Claims 28 and 37. Applicants therefore respectfully submit that independent Claims 28 and 37 are patentable over Ellison, Smeets, and Worley, alone or in any combination. Applicants respectfully request that the rejections of Claims 28 and 37 be withdrawn and that Claims 28 and 37 be allowed.

Accordingly, for at least the above reasons, Applicants respectfully submit that the Examiner's proposed combinations of Ellison, Smeets, and Worley fails to teach or disclose all

of the elements and limitations, and therefore the Claims as a whole, of Claims 22-38. As such, the Examiner's proposed combinations fail to establish a *prima facie* case for obviousness. Accordingly, the Examiner's rejections are insufficient, in error, and must also be withdrawn.

Based on all of the foregoing, Applicants respectfully submit that the Examiner's stated grounds are insufficient to maintain the Final Rejection. Applicants therefore respectfully request that the Final Rejections be withdrawn and that Claims 22-37 be allowed.

VIII. CLAIMS APPENDIX

See Attached.

IX. EVIDENCE APPENDIX

NONE.

X. RELATED PROCCEDINGS APPENDIX

NONE.

XI. CONCLUSION

For the foregoing reasons, Applicants respectfully submit that the Final Rejections of Claims 22-37 under 35 U.S.C. §103(a) are improper and should be reversed. Applicants respectfully request that the rejections of Claims 22-37 be withdrawn and that Claims 22-37 be allowed.

Respectfully submitted,

Dated: 23 February 2009

Patrick E. Caldwell, Esq.
Reg. No. 44,580
The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (972) 243-4523

VIII – APPENDIX – CLAIMS ON APPEAL

22. A secure processing system, comprising:

a main processor unit (MPU) coupled to a processor bus;

an attached processor complex (APC) coupled to the processor bus and comprising:

a local store configured to store computer instructions and data;

an attached processor unit (APU) coupled to the local store;

wherein the APC is configured to receive commands from the MPU via the processor bus, to store a cryptographic master key, and to operate in a non-isolated state and an isolated state; and

wherein in response to a LOAD command received from the MPU, the APC is configured to transition from the non-isolated state to the isolated state, to partition the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU, to transfer a set of computer instructions or data into the isolated section of the local store, and to use the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic key.

23. The secure processing system as recited in claim 22, wherein secure processing is performed within the isolated section of the local store of the APC.

24. The secure processing system as recited in claim 22, wherein the cryptographic master key stored in the APC is not accessible by the MPU.

25. The secure processing system as recited in claim 22, wherein the cryptographic master key stored in the APC is unique to the secure processing system.

26. The secure processing system as recited in claim 22, wherein when the APC is operating in the non-isolated state, the general access section occupies the entire local store.

27. The secure processing system as recited in claim 22, wherein when the APC is operating in the isolated state, the APC is configured to respond to an EXIT command received from the MPU by clearing the isolated section of the local store and eliminating the isolated section of the local store, thereby causing the general access section to occupy the entire local store.

28. The secure processing system as recited in claim 22, wherein the APC is configured to use the other cryptographic key to authenticate or decrypt another set of computer instructions or data.

29. The secure processing system as recited in claim 22, wherein the APC further comprises a bus interface unit (BIU) coupled to the processor bus, and wherein local store and the APU are coupled to the BIU.

30. The secure processing system as recited in claim 29, wherein the BIU comprises a load/exit state machine (LSEM) configured to store the cryptographic master key.

31. A method for carrying out secure processing, comprising:

providing a main processor unit (MPU), a processor bus, and an attached processor complex (APC), wherein the APC comprises a local store configured to store computer instructions and data and an attached processor unit (APU) coupled to the local store;

configuring the MPU to drive a LOAD command on the processor bus in the event secure processing is required;

coupling the MPU to the processor bus;

configuring the APC to receive the LOAD command via the processor bus, to store a cryptographic master key, and to operate in a non-isolated state and an isolated state;

configuring the APC to respond to a received LOAD command by:

transitioning from the non-isolated state to the isolated state;

partitioning the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU;

transferring a set of computer instructions or data into the isolated section of the local store;

using the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic key; and

coupling the APC to the processor bus.

32. The method as recited in claim 31, wherein the secure processing is carried out within the isolated section of the local store of the APC.

33. The method as recited in claim 31, wherein the cryptographic master key stored in the APC is not accessible by the MPU.

34. The method as recited in claim 31, wherein the coupling of the MPU and the APC to the processor bus forms a processing system, and wherein cryptographic master key stored in the APC is unique to the processing system.

35. The method as recited in claim 31, wherein when the APC is operating in the non-isolated state, the general access section occupies the entire local store.

36. The method as recited in claim 31, further comprising:

configuring the APC to respond to a received EXIT command when operating in the isolated state by:

clearing the isolated section of the local store; and

eliminating the isolated section of the local store, thereby causing the general access section to occupy the entire local store.

37. The method as recited in claim 31, wherein the configuring the APC to respond to a received LOAD command comprises:

configuring the APC to respond to a received LOAD command by:

transitioning from the non-isolated state to the isolated state;

partitioning the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU;

transferring a set of computer instructions or data into the isolated section of the local store;

using the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic; and

using the other cryptographic key to authenticate or decrypt another set of computer instructions or data.